Comparative Analysis of AES and RC4 Algorithms for Better Utilization

Nidhi Singhal[1], J.P.S.Raina[2]

Department of Electronics & Communication,
BBSB engineering college,
Fatehgarh Sahib,
Punjab,India

***Abstract*--In the today world, security is required to transmit confidential information over the network. Security is also demanding in wide range of applications. Cryptographic algorithms play a vital role in providing the data security against malicious attacks. But on the other hand, they consume significant amount of computing resources like CPU time, memory, encryption time etc. Normally, symmetric key algorithms are used over asymmetric key algorithms as they are very fast in nature. Symmetric algorithms are classified as block cipher and stream ciphers algorithms. In this paper, we compare the AES algorithm with different modes of operation (block cipher) and RC4 algorithm (stream cipher) in terms of CPU time, encryption time, memory utilization and throughput at different settings like variable key size and variable data packet size.**

***Keywords*-- Encryption, Decryption, Block and Stream Ciphers, AES, RC4**

I. Introduction

Cryptography is a science of secret writing. It is the art of protecting the information by transforming it into an unreadable format in which a message can be concealed from the casual reader and only the intended recipient will be able to convert it into original text .Cryptography renders the message unintelligible to outsider by various transformations. Data Cryptography is the scrambling of the content of data like text, image, audio and video to make it unreadable or unintelligible during transmission. Its main goal is to keep the data secure from unauthorized access [1]. Data that can be read and understood without any special measures is called plaintext or clear text. The method of disguising plaintext in such a way as to hide its substance is called encryption. Encrypting plaintext results in unreadable gibberish called cipher text. The process of reverting cipher text to its original plaintext is called decryption. A system that provides encryption and decryption is called cryptosystem. The simplicity or complexity of encryption process depends on encryption algorithm, software used and the key which is used in algorithm to encrypt or decrypt the data. Security of the encryption system depends on the security principle proposed by Kirchhoff. According to the Kirchhoff, the security of the encryption system should rely on the secrecy of the encryption /decryption key instead of the encryption algorithm itself. The security level of the encryption algorithm should depend on the size of the key space, secrecy of the key, length of the key, initialization vector and how they all work together.

Depending upon the number of keys used, cryptographic algorithms are classified as asymmetric algorithms (public key) and symmetric algorithms (secret key). Symmetric-key system uses a single key that both the sender and recipient have. Asymmetric-key system uses two keys, a public key known to everyone and a private key that only the recipient of messages uses. The symmetric key algorithms are further classified as block cipher (AES) and stream cipher (RC4). Block Ciphers operate with a fixed transformation on large blocks of plain text data while stream ciphers operate with the time varying transformation on individual plain text bits. Stream ciphers do not have a standard model and varieties of structures are followed in their design. Various benefits are quoted for stream cipher over block cipher like faster in operation, no or limited error propagation, low hardware complexity etc.

AES: The Advanced Encryption Standard (AES) was published by NIST (National Institute of Standards and Technology) in 2001. AES is a symmetric block cipher that is intended to replace DES as the approved standard for a wide range of applications. It has a variable key length of 128,192 or 256 bits. It encrypts data blocks of 128 bits in 10, 12, 14 rounds depending on key size. AES encryption is fast and flexible in block ciphers. It can be implemented on various platforms. AES can be operated in different modes of operation like ECB, CBC, CFB OFB, and CTR. In certain modes of operation they work as stream cipher.

RC4: RC4 is a stream cipher designed in 1987 by Ron Rivest. It is officially termed as "Rivest Cipher 4". Stream ciphers are more efficient for real time processing. It is a variable key size stream cipher with byte oriented operations. This algorithm is based on the use of a random permutation. According to the various analysis, the period of the cipher is greater than 10^{100}.Eight to sixteen machine operations are required per output byte and the cipher run very quickly in software. The algorithm is simple, fast and easy to explain. It can be efficiently implemented in both software and hardware.

II. Background and Related Work

To give more prospective in the field of cryptographic algorithms this section discusses the results obtained from various sources.

Different authors carried out extensive study in this regard. In reference [2] authors talks about different methods for evaluating the performance measure of RC2, DES, TDES, RC6, AES and Blowfish algorithms, all block cipher algorithms, on power consumption in terms of energy for wireless devices. The comparison is done in terms of power consumption, processing time and throughput. As the packet size of text files changes, with and without data transmission using different architecture and protocols, blowfish has better performance followed by RC6. TDES has low performance w.r.t DES. AES has better performance w.r.t RC2, DES, and TDES. RC2 is worst in all respects. Above results are valid for both encryption and decryption. Similar results were shown for audio files. In case of image files RC6 and Blowfish have disadvantage over other algorithms .when the data is transmitted there is insignificant difference between open key authentications and shared key authentication in ad hoc wireless LAN connection with excellent signals. For poor signals, transmission time gets increased over open sheered authentication in ad hoc mode. Similar results were presented in different papers by the same authors. In addition to the above results, they concluded that no significant difference was present when result was displayed in hex base encoding or base 64 encoding. Similar results were shown for video files. High key size leads to more battery and time consumption. As the throughput increases, power consumption decreases ([3]-[6]). In[7] author compares different algorithms of block cipher (AES, Serpent, Camellia, Cast-5, and Mars) on 8 bit microcontroller on ground of memory requirement, execution time and throughput. He concluded that AES is best in terms of memory requirement and throughput. Cast 5 and Camellia is an alternate for AES. Mars and serpent is poor w.r.t memory requirement and throughput.

Symmetric encryption ciphers are classified as stream cipher and block cipher. Stream ciphers do not have a standard model and various structures are used in their design. Various research works has been done in the area of stream ciphers and as a result various design models for stream ciphers were proposed. In [8] author gives the general idea about stream and block ciphers. While comparing both of them using RC4 and Hill cipher, he concluded that encryption and decryption speed of stream cipher is more than block cipher. Bit padding to the block cipher will add to more time and power consumption. In [9] Author compares different algorithms of stream cipher (Salsa 20, HC-128, VMPC, RC4, HC-256,Grain) and block cipher(IDEA , Blowfish, RC2, Serpent , Cast5 , RC6) on the ground of CPU time and throughput so that better algorithm can be used for network security in mobile devices. He concluded that stream ciphers are faster than block cipher. The performance of different algorithms can be checked on hardware platform. In [10], author talks about different structures and attacks on stream ciphers. A brief insight about the classification of stream cipher is also provided. They discuss different structural components used to design stream cipher. Till 2001 the only generic standards for stream ciphers were the block ciphers in different modes. Some application specific standards do exist. In general, many people think that there is no need for specific model and using block ciphers in stream cipher mode serve the purpose. Later it was found that many stream ciphers can be designed which are faster in S/Wand can be implemented in smaller H/W w.r.t. block ciphers. Moreover there security is better in some modes w.r.t their counterparts. Stream ciphers fulfill the requirements of multimedia applications of high throughput, low H/W complexity, and are technology specific.

III. Experimental Design

For our experiment, we use a laptop 2.99 GHz CPU and 2 GB RAM, in which performance data is collected. In the experiment, the laptop encrypts a different file size ranges from 100KB to 50MB.

In this work, we are trying to find out performance comparison between block cipher (AES) and stream cipher (RC4) algorithm. Based on the analysis and result, we will conclude that which algorithm is better to use based on different performance metrics.

Performance metrics are:

1) *Encryption time*- The encryption time is the time that an encryption algorithm takes to produce a cipher text from a plaintext. This time does not contain file I/O time.
2) *Decryption time*- The decryption time is the time that a decryption algorithm takes to produce a plaintext from a cipher text. This time does not contain file I/O time
3) *Throughput*-The *throughput* of an encryption scheme define the speed of encryption. The throughput is calculated as the total plaintext in Kilobytes encrypted/ encryption time (KB/sec).As the throughput increases, power consumption decreases.
4) *CPU process time*: The CPU process time is the time that a CPU is dedicated only to the particular process for calculations. It reflects the load of the CPU. More the CPU time used in the encryption process, the higher is the CPU load.
5) *Memory Utilization*: The Memory Utilization defines how much memory is being consumed while doing the encryption or decryption.

The above performance metrics are calculated based on following tasks:

i) Calculate the encryption and decryption time for each algorithm using different sizes input file.
ii) Compute the throughput for each algorithm in KB/Sec.

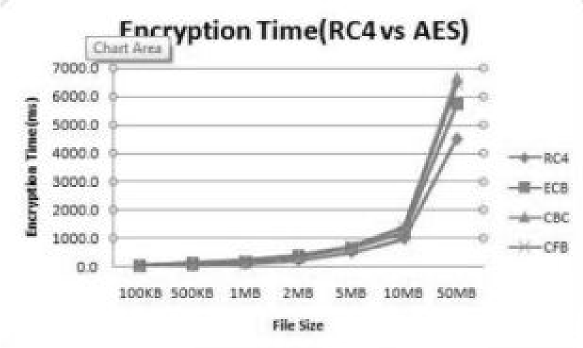
iii) The effect of changing the key size on encryption/decryption time.
iv) The effect of changing file size on memory utilization.
v) Calculate the CPU time for encryption and decryption for each algorithm using different sizes input file.

IV. Simulation Results

A. *The effect of changing packet size for cryptography algorithms on encryption and decryption time.*

a) *Encryption time based on different packet size*

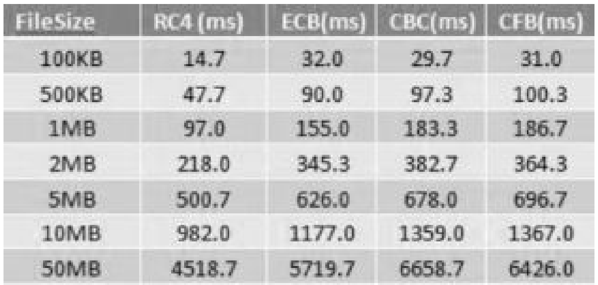
In Graph 1, we show the performance of cryptographic algorithms in terms of encryption time. Here, we compare the encryption time of AES and RC4 algorithm over different packet size. RC4 takes less time to encrypt files w.r.t. AES. In AES, CFB and CBC takes nearly similar time but ECB takes less time then both of these.



Graph.1: Encryption time of RC4 and AES

Table I

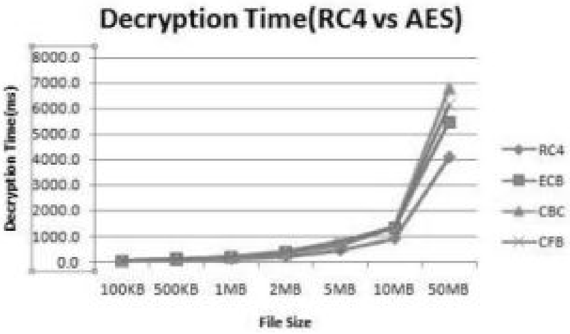
Encryption Time of RC4 and AES



FileSize	RC4 (ms)	ECB(ms)	CBC(ms)	CFB(ms)
100KB	14.7	32.0	29.7	31.0
500KB	47.7	90.0	97.3	100.3
1MB	97.0	155.0	183.3	186.7
2MB	218.0	345.3	382.7	364.3
5MB	500.7	626.0	678.0	696.7
10MB	982.0	1177.0	1359.0	1367.0
50MB	4518.7	5719.7	6658.7	6426.0

b) *Decryption time based on different packet size*

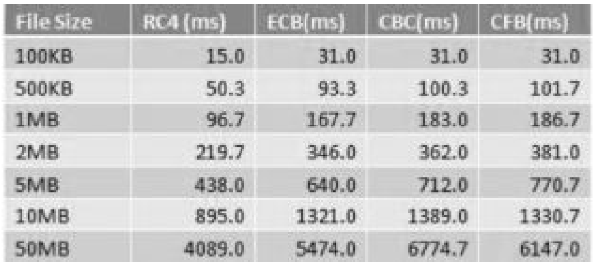
In Graph 2, we show the performance of cryptographic algorithms in terms of decryption time. Here, we compare the encryption time of AES and RC4 algorithm over different packet size. RC4 takes less time to decrypt files w.r.t. AES.



Graph.2: Decryption time of RC4 and AES

Table II

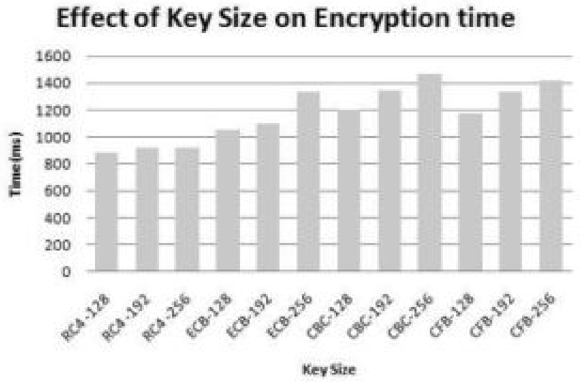
Decryption Time of RC4 and AES



File Size	RC4 (ms)	ECB(ms)	CBC(ms)	CFB(ms)
100KB	15.0	31.0	31.0	31.0
500KB	50.3	93.3	100.3	101.7
1MB	96.7	167.7	183.0	186.7
2MB	219.7	346.0	362.0	381.0
5MB	438.0	640.0	712.0	770.7
10MB	895.0	1321.0	1389.0	1330.7
50MB	4089.0	5474.0	6774.7	6147.0

c) *Encryption time based on different key size*

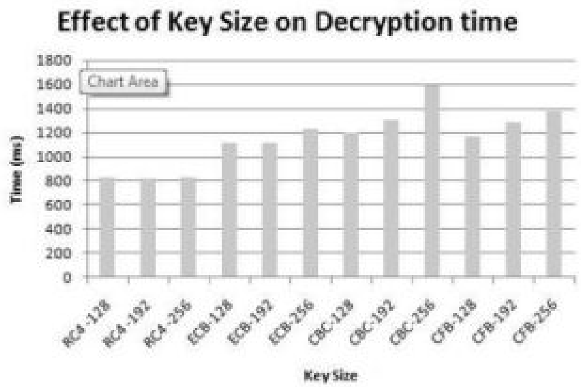
Another performance comparison point is the changing key size. The three different key sizes used are 128 bit, 192 bit and 256 bits. As the key size vary from 128 bits to 192 bits to 256 bits, encryption time for RC4 is almost constant and is less then AES. Hence it consumes less power w.r.t AES. But for different modes of AES, encryption time increases as key size increases.



Graph.3: Encryption time of RC4 and AES (with Key sizes)

d) *Decryption time based on different key size*

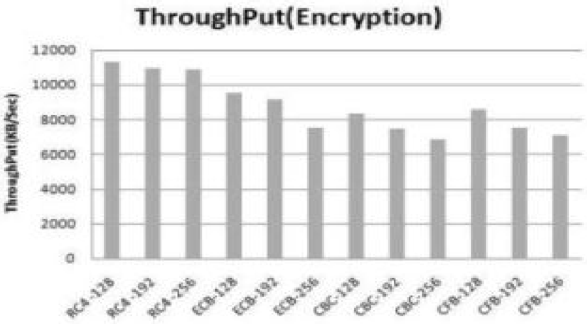
Better results were obtained in decryption w.r.t. encryption. And here also RC4 is better than AES.



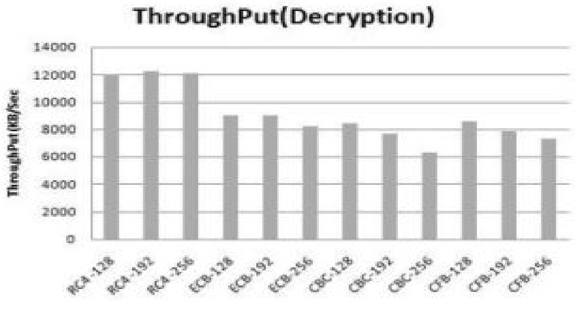
Graph.4: Decryption time of RC4 and AES (with Key sizes)

B. *Throughput for AES and RC4 with different key size*

Simulation results for this comparison point are shown in Graph 5 and 6. The result shows the superiority of RC4 over AES. With different key sizes RC4 gives almost the same result. But for different modes of AES, throughput decreases as key size increases because of more usage of computational power and encryption characteristics. Thus RC4 is fast in nature and consume less power w.r.t its counterparts. Better results were obtaining in decryption w.r.t. encryption.



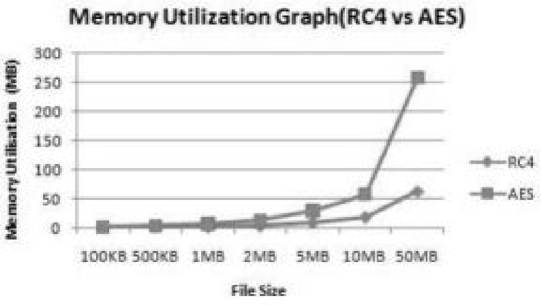
Graph.5 Encryption Throughput of RC4 and AES



Graph.6 Decryption Throughput of RC4 and AES

C. *The memory utilization for AES and RC4 with different file size*

Another most important performance parameter is the memory utilization. As per graph shown, AES consume more memory w.r.t.RC4 because of its characteristics. And as the file size increases memory size is drastically increased in AES means for extra large files, we need a system with good memory and more CPU.

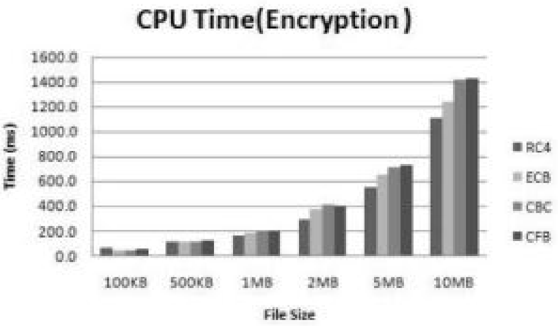


Graph.7 Memory utilization of RC4 and AES

D. *The effect of changing packet size for cryptography algorithms on CPU time.*

a) *Encryption of different packet size*

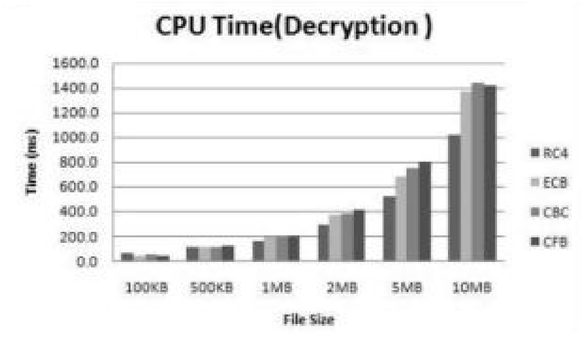
In Graph 8, we show the performance of cryptographic algorithms in terms of CPU process time. It reflects the CPU load. RC4 need more time to encrypt small size file w.r.t. its counterpart. AES need more time to encrypt large size files. Hence RC4 is useful for encrypting large data w.r.t AES. More over for large data, CFB and CBC takes nearly similar time but ECB takes less time then both of these. For small data, time needed by ECB and CBC is same.



Graph.8 Encryption CPU time of RC4 and AES

b) *Decryption of different packet size*

Graph 9 shows the experimental results for CPU process time during decryption. From the results we found that the results are nearly same as in the encryption process. And RC4 is better that AES.



Graph.9 Decryption CPU time of RC4 and AES

V. Conclusion

This work entitled "*Comparative Analysis of AES and RC4 Algorithms for Better Utilization*" presents a performance evaluation of RC4 and AES algorithms. The performance metrics were throughput, CPU process time, memory utilization, encryption and decryption time and key size variation. Experiments show that the RC4 is fast and energy efficient for encryption and decryption. Based on the analysis done as part of this research, RC4 is better than AES.

VI. Scope for Future Work

This work entitled "*Comparative Analysis of AES and RC4 Algorithms for Better Utilization*" presents a performance evaluation of RC4 and AES algorithms. Here we have considered only text file for comparison between AES and RC4 but based on same steps, we can compare the encryption algorithm based on video and audio files.

Acknowledgment

We would like to thanks R S Uppal, HOD, ECE, BBSB engineering College, Fathegarh Sahib as well as all ECE department of college for providing us a great help during this work.

References

[1] Alanazi Hamdan.O., Zaidan B.B., Zaidan A.A., Jalab Hamid.A., Shabbir .M and Al-Nabhani.Y, "New Comparative Study Between DES, 3DES and AES within Nine Factors" Journal of Computing, Volume 2, Issue 3, March2010, ISSN 2151-9617, pp.152-157 .

[2] Salama Diaa , Kader Hatem Abdual , and Hadhoud Mohiy , "Studying the Effects of Most Common Encryption Algorithms" International Arab Journal of e-Technology, Vol. 2, No. 1, January 2011, pp.1-10.

[3] Elminaam Diaa Salama Abdual., Kader Hatem Mohamed Abdual and Hadhoud Mohiy Mohamed,"Performance Evaluation of Symmetric Encryption Algorithms" IJCSNS International Journal of Computer Science and Network Security, VOL.8 ,No.12 , pp. 280-286, December 2008 .

[4] Elminaam Diaa Salama Abdual., Kader Hatem Mohamed Abdual and Hadhoud Mohiy Mohamed, "Tradeoffs between Energy Consumption and Security of Symmetric Encryption Algorithms" International Journal of Computer Theory and Engineering, Vol. 1, No. 3, pp. 325-333, August, 2009.

[5] Elminaam Diaa Salama Abdual., Kader Hatem Mohamed Abdual and Hadhoud Mohiy Mohamed, "Evaluating the Performance of Symmetric Encryption Algorithms" International Journal of Network Security, Vol.10, No.3,pp.213- 219, May 2010.

[6] Elminaam Diaa Salama Abdual., Kader Hatem Mohamed Abdual and Hadhoud Mohiy Mohamed, "Evaluating the Effects of Symmetric Cryptography Algorithms on Power Consumption for Different Data Types" International Journal of Network Security, Vol.11, No.2, pp.78- 87, Sept. 2010.

[7] Çakiroglu, Murat, "Software implementation and performance comparison Of popular block ciphers on 8-bit low-cost microcontroller" International Journal of the Physical Sciences, Vol. 5(9), pp. 1338-1343,August 2010.

[8] Ahmad Shish, Beg Mohd. Rizwan, Abbas Qamar , Ahmad Jameel and Atif Syed Mohd, "Comparative study between stream cipher and block cipher using RC4 and Hill Cipher" International Journal of Computer Applications(0975-8887),Vol.1,No.25, pp. 9-12.

[9] Sharif Suhaila Orner and Mansoor S.P., "Performance analysis of Stream and Block cipher algorithms" 3rd International Conference on Advanced Computer Theory and Engineering(ICACTE), 2010 IEEE, pp. V1-522 - V1-525.

[10] Bokhari, Mohammad Ubaidullah and Masoodi, Faheem, "Comparative Analysis of Structures And Attacks on Various Stream Ciphers" Proceedings of the 4th National Conference; INDIACom-2010.